

**IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE**

Garner J. Kohrell, individually and on)	
behalf of all others similarly situated,)	Case No. _____
)	
Plaintiff,)	JURY TRIAL DEMANDED
)	
Nelnet Servicing, LLC, and Edfinancial)	
Services, LLC,)	
)	
Defendants.)	

CLASS ACTION COMPLAINT

Plaintiff Garner J. Kohrell, (“Plaintiff”), upon personal knowledge of facts pertaining to him and on information and belief as to all other matters, by and through undersigned counsel, hereby brings this Class Action Complaint against Defendants Nelnet Servicing, LLC (“Nelnet”) and Edfinancial Services, LLC (“Edfinancial”) (collectively, “Defendants”), and alleges as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendants, who are student loan servicing companies, to seek damages for himself and other similarly situated current and former student loan borrowers (“borrowers”), or any other person(s) impacted in the data breach at issue (“Class Members”) who he seeks to represent, as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive information of Plaintiff and other Class Members. This action arises from Defendants’ failure to properly secure and safeguard personal identifiable information, including without limitation, unencrypted and unredacted names, addresses, email addresses, phone

numbers, and Social Security numbers (collectively, “personal identifiable information” or “PII”).

2. Plaintiff alleges Defendants failed to provide timely, accurate and adequate notice to Plaintiff and Class Members who were or are student loan borrowers whose PII was handled by Nelnet for the purpose of processing student loan payments. Current and former borrowers’ knowledge about what PII Defendants lost, as well as precisely what types of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by Defendants’ unreasonable notification delay after they first learned of the data breach.

3. On or about August 26, 2022, Nelnet notified state Attorney Generals about a widespread data breach involving sensitive PII of 2,501,324 individuals.¹ Nelnet explained in the required notice letter that it discovered an unauthorized third-party gained access to a portion of Nelnet’s system. Nelnet discovered that files on its network were accessed and acquired by the unauthorized actor (the “Data Breach”).

4. On July 21, 2022, Defendants chose not to notify affected borrowers or, upon information and belief, anyone, of their data breach, instead choosing to address the incident in-house by implementing other alleged, unspecified safeguards to some aspects of their computer security.

¹ Office of the Maine Attorney General, *Data Breach Notifications*, available at: <https://apps.web.maine.gov/online/aevviewer/ME/40/f6b4d5be-f7ef-412b-9966-e323ad6443a0.shtml> (last accessed September 6, 2022).

5. Approximately a month later, on August 17, 2022, Nelnet concluded its investigation and notified regulators and some Class Members that their PII had been impacted and was accessed on its network.² Additional Class Members, including Plaintiff, were notified on or after August 26, 2022, by additional loan servicing entities, such as Edfinancial, who use Nelnet as their servicing system and customer website portal provider.

6. According to the notice, Nelnet conducted an investigation to determine whether personal information hosted on its network may have been impacted as a result of the incident, and determined that Plaintiff's and Class Members' PII (including but not limited to full name and Social Security number) was impacted and stolen by the unauthorized person during the Data Breach.³

7. Plaintiff and the Class Members in this action were, upon information and belief, current and former student loan borrowers with their PII on Nelnet's system, serviced by Defendants and additional student loan servicers who use Nelnet as their servicing system and customer website portal provider. Upon information and belief, the first that Plaintiff and the Class Members learned of the Data Breach was when they received by U.S. Mail Notice of Data Breach letters on or after August 26, 2022.

8. In their Notice Letters, sent to Plaintiff and Class Members, Defendants failed to explain why they took over a month (from July 21, 2022, to August 26, 2022) to alert Class Members that their sensitive PII had been exposed. As a result of this delayed

² *Id.*

³ *Id.*

response, Plaintiff and Class Members were unaware that their PII had been compromised, and that they were, and continue to be, at significant risk to identity theft and various other forms of personal, social, and financial harm.

9. Plaintiff's and Class Members' unencrypted, unredacted PII was compromised due to Defendants' negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' sensitive data. Hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiff and similarly situated Class Members. The risks to these persons will remain for their respective lifetimes.

10. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect Plaintiff and Class Member PII; (ii) warn Plaintiff and Class Members of inadequate information security practices; and (iii) effectively monitor Nelnet's network for security vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

11. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their

accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach; (v) charges and fees associated with fraudulent charges on their accounts; and (vi) the continued and certainly an increased risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII. These risks will remain for the lifetimes of Plaintiff and Class Members.

12. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or at the very least negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, Plaintiff's and Class Members' PII was compromised through disclosure to an unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

13. Plaintiff Garrett Kohrell is a resident and citizen of Minnesota, residing in St. Paul. Plaintiff received a *Notice of Security Incident* from Edfinancial Services, LLC, on September 1, 2022, informing him his PII had been compromised in the Data Breach, dated August 26, 2022, by U.S. Mail.

14. Defendant Edfinancial Services, LLC is a student loan servicing company that has a principal place of business at 298 N Seven Oaks Drive, Knoxville, Tennessee 37922.

15. Defendant Nelnet Servicing, LLC is a student loan servicing company that has a principal place of business at 121 S. 13th Street, Suite 100, Lincoln, Nebraska 68508. Defendant Nelnet Servicing, LLC is a wholly-owned subsidiary of Nelnet Diversified Solutions LLC, which is itself a wholly-owned subsidiary of Nelnet Inc.

16. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

17. All of Plaintiff's claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

18. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

19. The Eastern District of Tennessee has personal jurisdiction over Defendants named in this action because Edfinancial is headquartered in this District and both

Defendants conduct substantial business in Tennessee and this District through their headquarters, offices, parents, and affiliates, and have continuous and systematic contact with the state of Tennessee. The Eastern District of Tennessee also has specific personal jurisdiction over Defendants related to this action because Plaintiff's claim arises out of Defendants' contacts with and student loan servicing business in this state and district.

20. Venue is proper in this District under 28 U.S.C. §1391(b) because Edfinancial is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

21. Edfinancial is a student loan servicing company that uses Nelnet, a different student loan servicing company, as its servicing system and customer website portal provider.

22. Both Edfinancial and Nelnet used identical language in their notice letters to Plaintiff and Class Members, claiming to take the privacy and security of customer information very seriously, stating, "The confidentiality, privacy, and security of our customers' information is one of our highest priorities."

23. Plaintiff and Class Members, as current or former student loan borrowers, reasonably relied (directly or indirectly) on these sophisticated student loan servicing companies to keep their sensitive PII confidential; to maintain system security; to use their information for business purposes only; and to make only authorized disclosures of their PII. Borrowers, in general, demand security to safeguard their PII, especially when financial information and other sensitive PII is involved.

24. Defendants had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

25. Both Defendants have privacy policies that discuss the importance of protecting and implementing reasonable measures to protect PII. Edfinancial's privacy policy (the "Edfinancial Privacy Policy") says "We are committed to excellence in customer service, and your privacy is important to us."⁴

26. The Edfinancial Privacy Policy further states:

The security of your personal information is important to us. When you enter sensitive information (such as a social security number) on our registration or order forms, we encrypt that information. We follow industry-accepted best practices for protecting personal information, both during transmission and at rest on our systems. While no method of communication over the Internet or electronic storage is ever 100% secure, we have gone to great lengths to protect your personal information through the use of firewalls, intrusion protection systems, file level encryption of data while at rest and encryption of data while in transit over our network. All systems provide extensive logging and automated reporting of issues enabling timely response, interdiction and corrective actions if necessary.⁵

27. The Edfinancial Privacy Policy also contains a forum selection clause that requires all claims arising from the privacy policy be conducted in state or federal court in Knox County, Tennessee.⁶

⁴ See <https://www.edfinancial.com/Privacy> (last accessed Sept. 6, 2022).

⁵ *Id.*

⁶ See *id.* ("This Privacy Policy shall be construed and governed under the laws of the United States and State of Tennessee (without regard to rules governing conflicts of laws provisions). You agree that venue for all actions, arising out of or relating in any way to your use of our Services, shall be in federal or state court of competent jurisdiction located in Knox County, Tennessee, within one (1) year after the claim arises. Each party waives any objections based on forum non conveniens and waives any objection to venue of any action instituted hereunder to the extent that an action is brought in the courts identified above.").

28. Nelnet’s privacy policy (the “Nelnet Privacy Policy”) states, “Protecting your privacy is important to Nelnet and our employees. . . .We implement reasonable and appropriate physical, procedural, and electronic safeguards to protect your information.”⁷

29. The Nelnet Privacy Policy does not permit Nelnet to use and disclose Plaintiff’s and Class Members’ PII unless complying with laws or to carry out internal functions.

30. The Nelnet Privacy Policy further states as follows:

Nelnet takes careful steps to safeguard customer information. We restrict access to your personal and account information to employees who need to know the information to provide services to you, and we regularly train our employees on privacy, information security, and their obligation to protect your information. We maintain reasonable and appropriate physical, electronic, and procedural safeguards to guard your Nonpublic Personal Information (NPI) and Personally Identifiable Information (PII), and we regularly test those safeguards to maintain the appropriate levels of protection.

31. Both of Defendants’ privacy policies explicitly state they apply to the PII at issue in the Data Breach, and to all personal information collected by Defendants from their websites, affiliates, and mobile apps.

32. Defendants violated their own privacy policies by unlawfully disclosing Plaintiff’s and Class Members’ Private Information to third parties.

33. On August 26, 2022, Defendants first began notifying state Attorneys General (“AGs”) and Class Members about a widespread data breach of Nelnet’s computer network involving the sensitive personally identifiable information of consumers.⁸

⁷ See <https://www.nelnet.com/privacy-and-security> (last accessed Sept. 6, 2022).

⁸ See *supra* note 1.

34. According to their Notice Letters to Class Members, Defendants explained that Nelnet discovered on July 21, 2022 (over a full month earlier) that it detected an unauthorized third-party gained access to a portion of their information systems and networks and notified Edfinancial that they had discovered vulnerabilities.

35. In notifying state AGs about the Data Breach on August 26, 2022, Nelnet disclosed that PII for 2,501,324 individuals was involved.

36. Defendants chose not to notify Plaintiff or Class Members of the Data Breach in July 2022, instead choosing to address the incident in-house by implementing other safeguards to some aspects of their computer security. They then simply resumed their normal business operations. Over a month later on August 26, 2022, Defendants admitted that Class Members' PII had been impacted and taken from their networks.

37. The notice letters Defendants sent Plaintiff and Class Members noted that the unauthorized actors had access to Nelnet's system from June through July 21, 2022, which is a very long time for an unauthorized actor to be permitted access to Plaintiff's and Class Members' PII while inside of Nelnet's system without detection. The notice letters provide no reason for the delay and no justification for preventing Plaintiff and Class Members from protecting their PII during the time in which Defendants chose not to notify Plaintiff and Class Members.

38. Nelnet "launched an investigation with third-party forensic experts" of Nelnet's systems, and determined that Plaintiff's and Class Members' personally identifiable information (including but not limited to full names and Social Security

numbers) was present and likely stolen by the unauthorized person at the time of the incident.

39. The notice letters sent to Plaintiff and Class Members noted unequivocally that their PII was impacted by the Data Breach.

40. Plaintiff and Class Members in this action were, upon information and belief, current and former student loan borrowers whose PII was utilized, stored, and maintained by Nelnet for purposes of servicing student loan payments. Plaintiff and Class Members first learned of the Data Breach when they received by U.S. Mail Notice of Data Breach letters dated August 26, 2022.

41. Upon information and belief, the PII was not encrypted prior to the Data Breach.

42. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and the Class Members. Defendants have made no indication to State AGs or to Plaintiff or Class Members that exfiltrated PII was retrieved from the cybercriminals who took it, or that all copies of exfiltrated data have been destroyed, and there is no reasonable way for Defendants to do so.

43. In response to the Data Breach, Nelnet claims it has further secured their systems to protect the private information. Nelnet admits additional security was required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward. Edfinancial has made no indications that it has further

secured systems to protect PII or to stop doing business with Nelnet or move information previously hosted by Nelnet to a different hosting system.

44. Defendants had obligations created by contract, industry standards, common law, and representations made to student loan borrowers to keep Plaintiff's and Class Members' PII confidential, and to protect the PII from unauthorized access and disclosure.

45. Plaintiff and Class Members provided their PII to Defendants with the reasonable expectation that Defendants, as sophisticated entities who do business with PII every day and who protect private, financial information, would comply with their duties, obligations and representations to keep such information confidential and secure from unauthorized access.

46. Defendants failed to uphold their data security obligations to Plaintiff and Class Members. As a result, Plaintiff and Class Members are significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

47. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining, causing Plaintiff's and Class Members' PII to be exposed.

48. Defendants could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII, and from only associating with entities that also properly encrypted and otherwise protected equipment and computer files containing PII.

49. In notice letters regarding the Data Breach, Defendants acknowledged the sensitive and confidential nature of the PII. To be sure, collecting, maintaining, and

protecting PII is vital to virtually all of Defendants' business purposes. Defendants acknowledged through their conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

50. It is well known that PII, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

51. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.⁹

52. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.¹⁰

53. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.¹¹

⁹ See https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed December 10, 2021).

¹⁰ *Id.*

¹¹ *Id.* at 15.

54. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes “significant negative financial impact on victims” as well as severe distress and other strong emotions and physical reactions.

55. Individuals are particularly concerned with protecting the privacy of their social security numbers, which are the “secret sauce” that is “as good as your DNA to hackers.”

56. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

57. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

58. Despite the prevalence of public announcements of data breach and data security compromises, and despite their own acknowledgments of data security compromises, and despite their own acknowledgment of their duties to keep PII private and secure, Defendants failed to take appropriate steps to protect Plaintiff and Class Members’ PII from being compromised.

59. At all relevant times, Defendants had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard

methods, train their employees, utilize available technology to defend their systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to *promptly* notify Plaintiff and Class Members when Defendants became aware that their customers' PII may have been compromised.

60. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class entrusted Defendants and/or their affiliates with their PII when they were student loan borrowers.

61. Defendants' duty also arises from the fact that they require their customers, including Plaintiff and Class Members, to use their online portals and websites to access and make payments for student loan debts incurred.

62. Defendants had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite their obligation to protect such information. Accordingly, Defendants breached their common law, statutory, and other duties owed to Plaintiff and Class Members.

63. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

- a. Maintaining a secure firewall configuration;
- b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;
- c. Monitoring for suspicious or irregular traffic to servers;

- d. Monitoring for suspicious credentials used to access servers;
- e. Monitoring for suspicious or irregular activity by known users;
- f. Monitoring for suspicious or unknown users;
- g. Monitoring for suspicious or irregular server requests;
- h. Monitoring for server requests for PII;
- i. Monitoring for server requests from VPNs; and
- j. Monitoring for server requests from Tor exit nodes.

64. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹² The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹³ The ramifications of Defendants’ failure to keep Plaintiff’s and Class Members’ PII secure are long lasting and severe. Once PII is stolen, particularly financial information and social security numbers, fraudulent use of that information and damage to victims is likely to continue for years.

65. Federal and state governments established security standards and issued recommendations to minimize unauthorized data disclosures, and the resulting harm to

¹² 17 C.F.R. § 248.201 (2013).

¹³ *Id.*

individuals and financial institutions. The FTC has promulgated numerous guides for businesses highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.¹⁴

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.¹⁵ Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹⁶

67. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious

¹⁴ Federal Trade Commission, *Start With Security: A Guide for Business*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed Feb. 15, 2022).

¹⁵ See Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Feb. 15, 2022).

¹⁶ *Id.*

activity on the network; and verify that third-party service providers have implemented reasonable security measures.

68. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.¹⁷

69. Through negligence in designing and implementing their computer systems and securing Plaintiff and Class Members’ PII, Defendants allowed thieves to access and collect individuals’ PII. Defendants failed to employ reasonable and appropriate measures to protect against unauthorized disclosure and access to Plaintiff and Class Members’ PII. Defendants’ data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

70. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data. The body of law created by the FTC

¹⁷ See Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, available at <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement> (last visited Feb. 15, 2022).

recognizes that failure to restrict access to information¹⁸ and failure to segregate access to information¹⁹ may violate the FTC Act.

71. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data, including personal information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

72. PII of data breach victims, like Plaintiff and Class Members, remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.²⁰ According to the Dark Web Price Index for 2021, payment card details for an account balance up to \$1,000 have an average market value of \$150, credit card details with an account balance up to \$5,000 have an average market value of \$240, stolen online banking logins with a minimum of \$100 on the account have an average market value of \$40, and stolen online banking logins with a minimum of \$2,000 on the account have an average market value of \$120.

¹⁸ *In the Matter of LabMD, Inc.*, Dkt. No. 9357, Slip Opinion, at 15 (“Procedures should be in place that restrict users’ access to only that information for which they have a legitimate need.”), available at <https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf>.

¹⁹ *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 258 (3d Cir. 2015) (companies should use “readily available security measures to limit access between” data storage systems).

²⁰ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed December 10, 2021).

73. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market.”

74. PII can be used to distinguish, identify, or trace an individual’s identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother’s maiden name.²²

75. Given the nature of Defendants’ Data Breach, as well as the delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff’s and Class Members’ PII may easily obtain Plaintiff’s and Class Members’ tax returns or open fraudulent credit card accounts in Class Members’ names.

76. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, basic credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.

77. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as dates of birth and social security numbers).

78. To date, Defendants have only offered Plaintiff and Class Members twenty-four months of credit monitoring services even with the month delay from their discovery of the Data Breach to the production of the notice letters. The advice offered to victims in the notice letters is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

79. Plaintiff's and Class Members' injuries were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Class Members.

80. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, contact information, financial information, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to: obtaining employment; obtaining a loan; applying for credit cards or spending money; filing false tax returns; stealing Social Security and other government benefits; and applying for a driver's license, passport, birth certificate, or other public document.

81. In addition, if a Class Member's Private Information is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

82. As a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been

deprived of the value of their PII, for which there is a well-established national and international market.

83. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.²¹

84. Accordingly, Defendants' wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud." Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

85. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages.

86. In the notice letter sent to Plaintiffs and Class Members, Defendants represented that they initially discovered the Data Breach in July 2022, and admitted

²¹ *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), <http://www.iii.org/insuranceindustryblog/?p=267> (last accessed December 10, 2021).

certain student loan registration information was accessed and acquired by the cybercriminals. As EmiSoft, an award-winning malware-protection software company, states “[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence, *especially during the preliminary stages of the investigation.*”²² It is likely that the cybercriminals did steal data and did so undetected.

87. In this case, according to Defendants’ notification to the Maine Attorney General, cybercriminals had access to Class Members’ data from June 1, 2022, yet their notice letters about that Data Breach did not go out until August 26, 2022.²³ This is tantamount to the cybercriminals having nearly a three-month head start on stealing the identities of Plaintiff and Class Members.

88. Accordingly, that Defendants have not found evidence of data being misused is not an assurance that the data were not accessed, acquired, and stolen. Indeed, the likelihood that cybercriminals stole the data covertly is significant, likely, and concerning.

89. Plaintiff provided his personal information to Nelnet and/or its affiliate Edfinancial as a requirement with servicing related to Plaintiff’s student loans.

90. As part of his involvement with Defendants, Plaintiff entrusted his PII, and other confidential information such as name, address, Social Security number, phone number, financial account information, and other personally identifiable information with the reasonable expectation and understanding that Nelnet and Edfinancial would take at a

²² EmiSoft Malware Lab, *The chance of data being stolen in a ransomware attack is greater than one in ten* (EMISOFT BLOG July 13, 2020), <https://blog.emissoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/> (last accessed December 13, 2021, emphasis added)).

²³ See supra note 1.

minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized use or disclosure, and would timely notify him of any data security incidents related to him. Plaintiff would not have permitted his PII to be given to Defendants had he known it would not take reasonable steps to safeguard his PII.

91. On or about September 1, 2022, nearly three months after the Data Breach began, Plaintiff received a letter notifying him that his PII had been improperly accessed and taken by unauthorized third parties. The notice indicated that Plaintiff's PII was compromised as a result of the Data Breach.

92. As a result of the Data Breach, Plaintiff has or will make reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or personal records for any indications of actual or attempted identity theft or fraud. Plaintiff froze his credit and took proactive steps immediately upon receiving notice of the Data Breach.

93. Plaintiff spent this time at Defendants' direction. Indeed, in the Notice letter Plaintiff received, Defendants directed Plaintiff to take steps to mitigate his losses:

We encourage you to remain vigilant against incidents of identity theft and fraud over the next 24 months, by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "Steps You Can Take to Help Protect Your Personal Information."

94. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendants obtained from Plaintiff; (b) violation of his privacy

rights; (c) the theft of his PII; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

95. As a result of the Data Breach, Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. The Data Breach has caused Plaintiff to suffer significant fear, anxiety, and stress, which has been compounded by the fact that his Social Security number and other intimate details are in the hands of criminals.

96. As a result of the Data Breach, Plaintiff anticipates spending considerable time and/or money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

97. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

98. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated.

99. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All persons residing in the United States whose PII was compromised in the 2022 data breach announced by Nelnet Servicing, LLC in August 2022 (the “Nationwide Class”).

100. Excluded from the Nationwide Class are the following individuals and/or entities: Defendants and Defendants’ parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

101. Plaintiff reserves the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

102. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are at least 2,501,324 individuals whose Private Information may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendants’ records.

103. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exists and predominates over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendants had a duty to protect Plaintiff's and Class Members' PII;
- b. Whether Defendants had duties not to disclose the Plaintiff's and Class Members' PII to unauthorized third parties;
- c. Whether Defendants had duties not to use Plaintiff's and Class Members' PII for non-business purposes;
- d. Whether Defendants failed to adequately safeguard Plaintiff's and Class Members' PII;
- e. Whether and when Defendants actually learned of the Data Breach;
- f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
- h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII;

- k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;
- l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and
- m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

104. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendants' misfeasance.

105. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

106. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the

infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intend to prosecute this action vigorously.

107. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

108. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will

establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

109. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

110. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

111. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure and unlawful disclosure of the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

112. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

113. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether a contract existed between Defendants on the one hand, and Plaintiff and Class Members on the other, and the terms of that contract;
- e. Whether Defendants breached the contract;
- f. Whether an implied contract existed between Defendants on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;
- g. Whether Defendants breached the implied contract;
- h. Whether Defendants adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;
- i. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII;

- k. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I

Negligence

(On Behalf of Plaintiff and the Nationwide Class)

114. Plaintiff restates and realleges all of the foregoing paragraphs as if fully set forth herein.

115. As a condition of having their student loans processed, Plaintiff and Class Members, as current and former student loan borrowers, are obligated to provide Defendants with certain PII, including but not limited to, their name, date of birth, address, Social Security number, state-issued identification numbers, tax identification numbers, military identification numbers, and financial account numbers.

116. Plaintiff and Class Members entrusted their PII to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII for legitimate business purposes only, and/or not disclose their PII to unauthorized third parties.

117. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

118. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and/or using of the PII involved an unreasonable

risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

119. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing security protocols to ensure that Plaintiff's and Class Members' information in Defendants' possession was adequately secured and protected.

120. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

121. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Defendants' business as a sophisticated student loan service provider, for which the diligent protection of PII is a continuous forefront issue.

122. Plaintiff and Class Members were the foreseeable and probable victims of Defendants' inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems.

123. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the

safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to Defendants.

124. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, Defendants' possession; only Defendants had the ability.

125. Defendants were in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

126. Defendants had and continue to have a duty to adequately and promptly disclose that Plaintiff's and Class Members' PII within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

127. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of Plaintiff's and Class Members' PII.

128. Defendants have admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

129. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII during the time the PII was within Defendants' possession or control.

130. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation

PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

131. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendants failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

132. Defendants improperly and inadequately safeguarded Plaintiff's and Class Members' PII in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

133. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect borrower PII in the face of increased risk of theft.

134. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

135. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

136. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII would not have been compromised.

137. There is a close causal connection between Defendants' failure to implement security measures to protect Plaintiff's and Class Members' PII and the harm suffered or risk of imminent harm suffered by Plaintiff and Class. Plaintiff's and Class Members' PII was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

138. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

139. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

140. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

141. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

142. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against

businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class.

143. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Defendants' goods and services they received.

144. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm,

including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

145. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

COUNT II

Unjust Enrichment

(On Behalf of Plaintiff and the Nationwide Class)

146. Plaintiff re-alleges and incorporates by reference paragraphs above as if fully set forth herein.

147. Plaintiff and Class Members conferred a monetary benefit on Defendants and their affiliate student loan companies in the form of monetary payments—directly or indirectly—for providing student loan services to current and former borrowers.

148. Defendants collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendants had knowledge of the monetary benefits they received on behalf of the Plaintiff and Class Members.

149. The money that borrowers paid to Defendants should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII.

150. Defendants failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

151. As a result of Defendants’ failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiff and Class Members suffered actual damages in an amount of the savings and costs Defendants reasonably and contractually should have expended on data security measures to secure Plaintiff’s PII.

152. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendants failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiff’s and Class Members’ PII and that the borrowers paid for.

153. As a direct and proximate result of Defendants’ decision to profit rather than provide adequate security, and Defendants’ resultant disclosures of Plaintiff’s and Class Members’ PII, Plaintiff and Class Members suffered and continue to suffer considerable injuries in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, and a present increased risk of harm.

COUNT III

Breach of Express Contract

(On Behalf of Plaintiff and the Nationwide Class)

154. Plaintiff re-alleges and incorporates by reference the above paragraphs as if fully set forth herein.

155. This count is pleaded in the alternative to Count II (Unjust Enrichment) above.

156. Plaintiff and Class Members allege that they were the express, foreseeable, and intended beneficiaries of valid and enforceable express contracts between Defendants and their former and current customers, contract(s) that (upon information and belief) include obligations to keep sensitive PII private and secure.

157. Upon information and belief, these contracts included promises made by Defendants that expressed and/or manifested intent that the contracts were made to primarily and directly benefit the Plaintiff and the Class (all customers entering into the contracts), as Defendants' service was for student loan services for Plaintiff and the Class, but also safeguarding the PII entrusted to Defendants in the process of providing these services.

158. Upon information and belief, Defendants' representations required Defendants to implement the necessary security measures to protect Plaintiff's and Class Members' PII.

159. Defendants materially breached their contractual obligation to protect the PII of Plaintiff and Class Members when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

160. The Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

161. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure of their PII, the loss of control of their PII, the present risk of suffering additional damages, and out-of-pocket expenses.

162. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT IV

Breach of Implied Contract

(On Behalf of Plaintiff and the Nationwide Class)

163. Plaintiff re-alleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

164. This count is plead in the alternative to Count II (Unjust Enrichment) above.

165. Plaintiff's and Class Members' PII was provided to Defendants as part of student loan services that Defendants provided to Plaintiff and Class Members.

166. Plaintiff and Class Members agreed to pay Defendants for their services.

167. Defendants and the Plaintiff and Class Members entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the security of Plaintiff's and Class Members' PII, whereby,

Defendants were obligated to take reasonable steps to secure and safeguard Plaintiff's and Class Members' PII.

168. Defendants had an implied duty of good faith to ensure that the PII of Plaintiff and Class Members in their possession was only used in accordance with their contractual obligations.

169. Defendants were therefore required to act fairly, reasonably, and in good faith in carrying out their contractual obligations to protect the confidentiality of Plaintiff's and Class Members' PII and to comply with industry standards and applicable laws and regulations for the security of this information.

170. Under these implied contracts for data security, Defendants were further obligated to provide Plaintiff and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

171. Defendants breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII, resulting in the Data Breach.

172. Defendants further breached the implied contract by providing untimely notification to Plaintiff and Class Members who may already be victims of identity fraud or theft or are at present risk of becoming victims of identity theft or fraud.

173. The Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

174. As a result of Defendants' conduct, Plaintiff and Class Members did not receive the full benefit of the bargain.

175. Had Defendants disclosed that their data security was inadequate, neither the Plaintiff or Class Members, nor any reasonable person would have entered into such contracts with Defendant.

176. As a result of Data Breach, Plaintiff and Class Members suffered actual damages resulting from the theft of their PII, as well as the loss of control of their PII, and remain at present risk of suffering additional damages.

177. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

178. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT V

Invasion of Privacy

(On Behalf of Plaintiff and the Nationwide Class)

179. Plaintiff re-alleges and incorporates by reference all other allegations in the Complaint as if fully set forth herein.

180. Plaintiff and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored, and maintained by Defendants, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access and publication of their PII to criminal actors, as occurred with the

Data Breach. The PII of Plaintiff and Class Members contain intimate details of a highly personal nature, individually and in the aggregate.

181. Plaintiff and Class Members reasonably expected that Defendants would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

182. Defendants intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party.

183. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia: intruding into their private affairs in a manner that would be highly offensive to a reasonable person; invading their privacy by improperly using their PII obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons; failing to adequately secure their PII from disclosure to unauthorized persons; and enabling the disclosure of their PII without consent.

184. This invasion of privacy resulted from Defendants' intentional failure to properly secure and maintain Plaintiff's and Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

185. Plaintiff and Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiff's,

and Class Members' PII, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

186. The disclosure of Plaintiff's and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

187. Defendants' willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiff's and Class Members' intimate and sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

188. The unauthorized access, exfiltration, and disclosure of Plaintiffs' and Class Members' PII was without their consent, and in violation of various statutes, regulations and other laws.

189. As a direct and proximate result of Defendants' intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against Defendants and that the Court grant the following:

- A. For an Order certifying the Nationwide Classes and appointing Plaintiff and his Counsel to represent the certified Nationwide Class;
- B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's

and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiff and Class;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including but not limited to an order:

- i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
- ii. requiring Defendants to protect, including through encryption, all data collected through the course of their businesses in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
- iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class;
- iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;
- v. prohibiting Defendants from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

- vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;
- ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' networks are compromised, hackers cannot gain access to other portions of Defendants' systems;
- x. requiring Defendants to conduct regular database scanning and securing checks;
- xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

- xii. requiring Defendants to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and
- xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis

to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

xviii. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

D. For an award of punitive damages;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated: September 8, 2022

Respectfully submitted,

/s/ J. Gerard Stranch, IV

J. Gerard Stranch, IV (TN Bar #023045)

**BRANSTETTER, STRANCH &
JENNINGS, PLLC**

223 Rosa L. Parks Avenue, Ste. 200

Nashville, TN 37203

Tel: 615-254-8801

Email: gerards@bsjfirm.com

Peter J. Jannace (KY Bar #95964)*

**BRANSTETTER, STRANCH &
JENNINGS, PLLC**

515 Park Avenue

Louisville, KY 40208

Tel: 502-636-4333
Email: peterj@bsjfirm.com

Kate M. Baxter-Kauf (MN #0392037)*
Karen Hanson Riebel (MN #0219770)*
Maureen Kane Berg
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com
mkberg@locklaw.com

**Pro Hac Vice applications forthcoming*

Attorneys for Plaintiffs and the putative Class